AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE

NAMING AND PROFILES DOCUMENT

VERSION 09

Contents

A. Introduction

TunTrust is a certification authority (CA) that issues digital certificates in accordance with its CP/CPS published in the website http://www.tuntrust.tn/repository. As a CA, TunTrust performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

TunTrust is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described in the TP/TPS published in the website http://www.tuntrust.tn/repository.

This document has been modified as follows:

Version	Date	Comment	Section/Page
00	20/02/2017	1st Writing	Whole document
01	31/08/2018	2nd Writing	Whole document
02	14/09/2018	3rd Writing	Sections Timestamp request format and Timestamp response format
03	28/12/2018	4th revision	Section F.1 ID-Trust
04	26/01/2019	5th revision	Section F.1 ID-Trust
05	06/02/2019	6th revision	Section F.1 ID-Trust
06	08/03/2019	7th revision	Section D.1 and F.1
07	13/09/2019	8th revision	Section F.3
08	15/11/2019	9th revision	Sections E.2, E.3 and E.4
08.1	13/01/2020	10th revision	B.2, F.1 and F.3
08.2	22/06/2020	11th revision	Add section E.5 & modify section F.3
08.3	28/08/2020	Modify validity periods of certificates & add clarifications	D.1 and G
08.4	10/11/2020	Modify validity period of DigiGO Advanced	E.5
08.5	01/12/2020	Omit the OU field from OV SSL certifiates	D.1
08.6	27/07/2021	Add Enterprise ID-C40	E6 & F2
08.7	28/09/2021	Add Pass-sanitaire profiles	B-2, B-3, B-4, E-7, H, C-8, G-1, G-2 & H-1
08.8	07/02/2022	Change Subject DN in H.1	Header, Footer, section H.1
08.9	18/07/2022	Sunset issuing OV SSL Certificates with TunServerCA2 & add Mobile-ID & decrease the validity period of 2D-DOC Certificates	Section B.1, C.1, C.2, D.1 & G.1
09	16/05/2024	Modify UXP Profiles	Sections E.2 & E.3

B. TunTrust CAs Hierarchies

- TunTrust, acting as TSP is using several Certification Authorities (CAs), as shown in the certificates hierarchy, to issue TunTrust end-users certificates:Two level CA hierarchy (figure 1) to issue OV SSL Certificate
- Three level CA hierarchy (figure 2) to issue Digital Signature Certificate, e-Seal Certificate, DigiGO Certificate and Mobile-ID Certificate.
- One level CA hierarchy (figure 3) to issue visible digital seal certificate and Upload certificate.
- One level CA hierarchy (figure 4) to issue the DSC certificates as part of the “pass-sanitaire” project.

1. Tunisian Root Certificate Authority – TunRootCA2

ThisTunTrust CA hierarchy consists of the following CAs (see figure 1):

- One TunRootCA2 self-signed root and kept offline.
- One issuing CA: TunServerCA2 root-signed by ***TunRootCA2*** and operates online to issue OV SSL certificates.

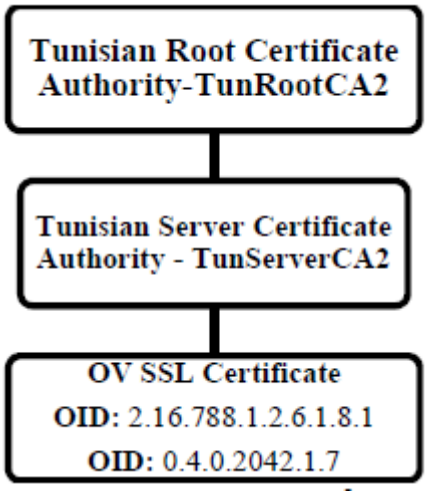

Figure 1- TunRootCA2 hierarchy

TunTrust has not issued OV SSL Certificates with this hierarchy of CAs as of December 31st , 2021 and will not issue any until it expires.

2. Tunisia National Root CA

The Tunisian National PKI hierarchy consists of the following CAs (see figure 1):

- One **Tunisia National Root CA** self-signed root and kept offline.
- Two intermediate CAs:
  - **Tunisia Gov CA**: is a root-signed Tunisia National Root CA and kept offline.
  - **Tunisia Corporate CA**: is a root-signed Tunisia National Root CA and was revoked on the 08th of August 2018.
- Four Issuing CAs:
  - **TnTrust Gov CA**: is a CA signed by Tunisia Gov CA and operates online to issue LCP certificates.
  - **TnTrust Qualified Gov CA** : is a CA signed by Tunisia Gov CA and operates online to issue QCP-n-qscd and QCP-l-qscd certificates
  - **TnTrust Corporate CA**: is a CA signed by Tunisia Corporate CA and was revoked on August, 08, 2018.
  - **TnTrust Qualified Corporate CA**: is a CA signed by Tunisia Corporate CA and was revoked on the 08th of August 2018.

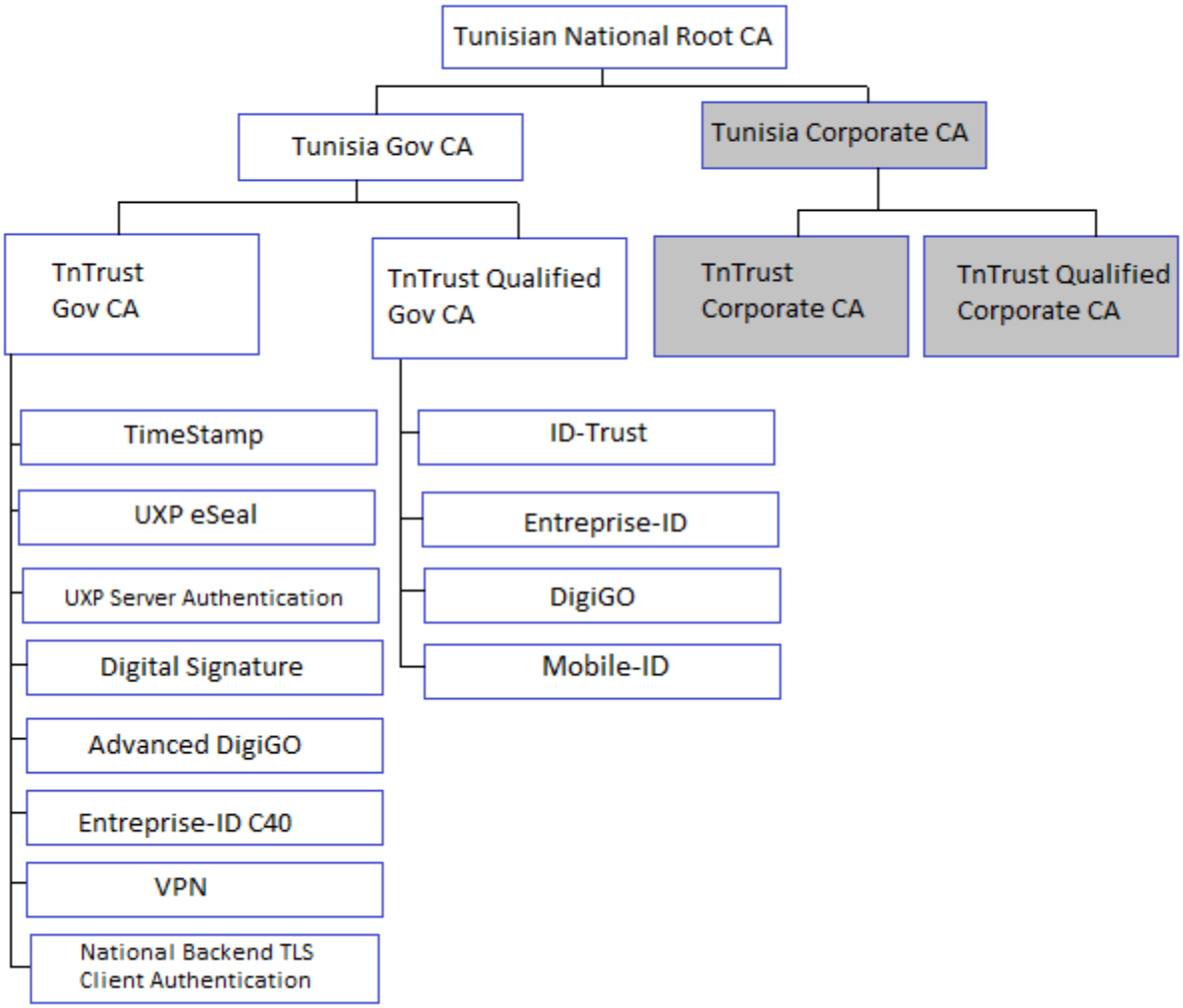

Figure -2 Tunisia National Root CA hierarchy

3. TN01

The TN01 CA is a self-signed root CA that delivers the e-seal certificates and Upload certificates.

1. E-seal certificate is a Visible Digital Seal to ensure the authenticity of certain types of documents as well as the integrity and conformity of the copies made compared to their original version. In this context, TunTrust issues e-seal certificates that comply with the technical requirements of the 2D-DOC standard v 3.0.0.
2. Upload certificate profile was created as part of the “pass-sanitaire” project. The usage purpose of this certificate is the digital signature.

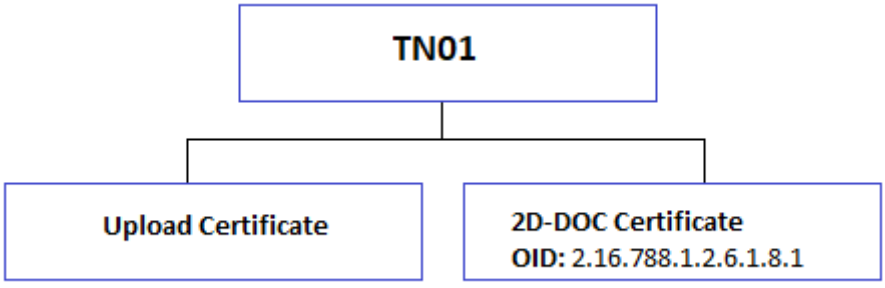

Figure 3- 2DDOC CA hierarchy

4. CSCA TUNISIA DGC

The CSCA TUNISIA DGC CA is a self-signed root CA that delivers the DSCs certificates as part of the “pass-sanitaire” project.

Figure 4- Digital Green Pass Hierarchy

C. Certification Authorities Profiles

1. Tunisian Root Certificate Authority - TunRootCA2

The following table describes the TunRootCA2 certificate profile, however no Certificate has been issued using this CA since December 31st 2021

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		2166150505270505BC8AB01DAF0ABEC4
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Subject DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Validity	X		
Not Before	X		5 May 2015 09:57:01
Not After	X		5 May 2027 09:57:01
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
X509v3 Subject Key Identifier	X		CC:73:C5:A3:6A:29:31:97:A7:8D:A0:D8:54 :C1:0A:75:B6:23:3F:A6
X509v3 Basic Constraints	X	True	CA:TRUE
KeyUsage	X	True	
Certificate Sign			Set
CRL Sign			Set

2. Tunisian Server Certificate Authority - TunServerCA2

The following table describes TunServerCA2 certificate profile however no Certificate has been issued using this CA since December 31st 2021:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		216615050625050514681E592CF41849

Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		O = National Digital Certification Agency, CN = Tunisian Root Certificate Authority - TunRootCA2, C=TN
Subject DN	X		CN = Tunisian Server Certificate Authority - TunServerCA2, O = National Digital Certification Agency, C = TN
Validity			
Not Before	X		7 May 2015 01:00:00
Not After	X		8 May 2025 00:59:59
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://ocsp.certification.tn CA Issuers - URI: http://www.certification.tn/pub/TunRootCA2.crt
X509v3 Subject Key Identifier	X		87:AB:F7:69:4B:50:F6:61:57:FF:3F:5B:8E:1D:70:C6:A2:6C:AA:C6
X509v3 Basic Constraints	X	True	CA:TRUE pathlen:0
X509v3 Authority Key Identifier	X		CC:73:C5:A3:6A:29:31:97:A7:8D:A0:D8:54:C1:0A:75:B6:23:3F:A6
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/TunRootCA2.crl
Key Usage	X	True	
Certificate Sign			Set
CRL Sign			Set
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.8.1 CPS: https://www.certification.tn/cps User Notice: Organization: National Digital Certification Agency Number: 1 Explicit Text: https://www.certification.tn/rpa

3. Tunisia National Root CA

The following table describes the Tunisia National Root CA Certificate profile:

Base Profile	Included	Critical	Values

Version	X		V3
Serial Number	X		68:3E:11:55:92:9C:8E:8E
Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Validity	**X**		
Not Before	X		Nov 29 09:02:56 2016 GMT
Not After	X		May 29 09:02:56 2037 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8:7E:1C:6F:14:08:8E
X509v3Authority Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8:7E:1C:6F:14:08:8E
X509v3 Private Key Usage Period	X		Not Before: Nov 29 09:02:56 2016 GMT, Not After: May 29 09:02:56 2037 GMT
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunrootca.crl
X509v3 Basic Constraints	X	True	CA:TRUE
X509v3 Key Usage	**X**	**True**	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

4. Tunisia Gov CA

The following table describes the Tunisia Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		78:2C:10:09:83:0A:4B:EE

Signature Algorithm			
Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia National Root CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Validity	**X**		
Not Before	X		Nov 29 09:35:15 2016 GMT
Not After	X		Feb 29 09:35:15 2032 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 4096 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C:42:D3:B7:B8:B9:46
X509v3Authority Key Identifier	X		0E:BE:D1:48:44:12:52:23:2B:47:14:FA:5F:A8:7E:1C:6F:14:08:8E
X509v3 Private Key Usage Period	X		Not Before: Nov 29 09:35:15 2016 GMT, Not After: Feb 29 09:35:15 2032 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.9
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunrootca.crl
X509v3 Basic Constraints	X	True	CA:TRUE
Key Usage	**X**	**True**	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

5. TnTrust Gov CA

The following table describes the TnTrust Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		36:71:6F:A4:36:EC:C2:D2
Signature Algorithm			

Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Validity	**X**		
Not Before	X		Nov 29 10:47:01 2016 GMT
Not After	X		Dec 29 10:47:01 2026 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 3072 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		7B:D6:C4:15:45:CF:06:34:95:69:36:86:DA:75:7D:9B:FB:EB:73:D9
X509v3Authority Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C:42:D3:B7:B8:B9:46
X509v3 Private Key Usage Period	X		Not Before: Nov 29 10:47:01 2016 GMT, Not After: Dec 29 10:47:01 2026 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.9
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunisiagovca.crl
X509v3 Basic Constraints	X	True	CA:TRUE Pathlen : 0
Key Usage	X	True	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

6. TnTrust Qualified Gov CA

The following table describes the TnTrust Qualified Gov CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		
Signature Algorithm			

Algorithm	X		SHA256 with RSA Encryption
Signature Value	X		CA Signature
Issuer DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=Tunisia Gov CA
Subject DN	X		C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Gov CA
Validity	**X**		
Not Before	X		Nov 29 10:24:02 2016 GMT
Not After	X		Dec 29 10:24:02 2026 GMT
SubjectPublicKeyInfo	X		Public Key: Key length: 3072 bits (RSA) Exponent: 65537 (0x10001)
X509v3 extensions			
Authority Information Access	X		OCSP - URI:http://va.certification.tn
X509v3 Subject Key Identifier	X		73:24:28:25:FA:22:F6:92:A9:15:83:A4:2C:B3:CD:C6:CB:B4:03:56
X509v3Authority Key Identifier	X		AF:81:94:4C:7B:36:7A:6D:F8:9B:12:94:55:9C:42:D3:B7:B8:B9:46
X509v3 Private Key Usage Period	X		Not Before: Nov 29 10:24:02 2016 GMT, Not After: Dec 29 10:24:02 2026 GMT
X509v3 Certificate Policies	X		Policy: 2.16.788.1.2.6.1.10
X509v3 CRL Distribution Points	X		URI:http://crl.certification.tn/tunisiagovca.crl
X509v3 Basic Constraints	X	True	CA:TRUE Pathlen : 0
Key Usage	**X**	**True**	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

7. TN01

The following table describes the TN01 CEV CA certificate profile:

Base Profile	Included	Critical	Values
Version	X		V3
Serial Number	X		6A:B8:26:4E:06:82:56:97
Signature Algorithm			

Algorithm	X		ecdsa-with-SHA256
Signature Value	X		CA Signature
Issuer DN	X		CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Subject DN	X		CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Validity	**X**		
Not Before	X		Apr 27 12:52:57 2017 GMT
Not After	X		Apr 27 12:52:57 2027 GMT
ASN1 OID	X		secp384r1
X509v3 extensions			
X509v3 Subject Key Identifier	X		CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2:8A:9C:58
X509v3Authority Key Identifier	X		CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2:8A:9C:58
X509v3 Basic Constraints	X	True	CA:TRUE
Key Usage	X	True	
Digital Signature			Set
Certificate Sign			Set
CRL Sign			Set

8. CSCA TUNISIA DGC

The following table describes the CSCA TUNISIA DGC certificate profile:

Base Profile	Critical	Values
Version		3 (0x2)
Serial Number		To be defined
Signature Algorithm		ecdsa-with-SHA256
Issuer		CN=CSCA TUNISIA DGC, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Subject		CN=CSCA TUNISIA DGC, O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE, C=TN
Validity		
Not Before		Issuance date
Not After		Issuance date + **4 years**

X509v3 Private Key Usage Period		Not Before: issuance date, Not After: issuance date + 1 year
Subject Pubic Key Info		
Public Key Algorithm		id-ecPublicKey
id-ecPublicKey		384 bit
pub		To be identified
X509v3 extensions		
X509v3 Subject Key Identifier		To be identified
X509v3 Authority Key Identifier		To be identified
X509v3 Basic Constraints	True	CA: TRUE pathlen : 0
X509 Key Usage	True	Certificate Sign, CRL Sign

D. TunServerCA2 End-Entity Certificates Profiles

The following type of Certificates were issued under TunServerCA2 CA until December 31st 2021:

1. OV SSL Certificates

TunTrust OV SSL Server Certificates are ETSI EN 319 411-1 Certificates not certified as generated on QSCD, with creation of the keys by the Subscriber, with 2048-bit key size and a one (1) year validity period.
These TunTrust SSL Certificates are compliant with and include the OID reference of the OVCP certificate policy of the ETSI Technical Standard 319 411-1 (i.e., 0.4.0.2042.1.7).
The usage purpose of these TunTrust SSL Certificates is the combined purpose of digital signature and key encryption.
The TunTrust OVCP Server Certificates include the corresponding TunTrust OID for SSL server certificates, i.e., *<2.16.788.1.2.6.1.8 >*.
The following table provides the description of the fields for TunTrust OV SSL Certificates issued under TunServerCA2:

Base Profile	Included	Critical	O/M[1]	CO[2]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	TunServerCA2 Signature
Issuer DN	X			S	C=TN, O=National Digital Certification Agency, CN=Tunisian Server Certificate Authority - TunServerCA2
Subject DN	X	False			
serialNumber	X		M	D	Serial Number as constructed by CRAO
commonName	X		O	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
localityName	X		M	D	Location in which the company's registered office is established.
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
emailAddress	X		O	D	Email Address
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 365 days
subjectPublicKeyInfo	X	False			

1O/M: O = Optional, M = Mandatory.
2 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				keyid:87:AB:F7:69:4B:50:F6:61:57:FF:3F:5B:8E:1D:70:C6:A2:6C:AA:C6
authorityInfoAccess	X	False			
Authority Information Access	X				CA Issuers - URI:http://www.tuntrust.tn/pub/TunServerCA2.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/TunServerCA2.crl
subjectAltName	X	False			
SubjectAltName-dNSName[3]	X		M		FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	False
KeyEncipherment	X			S	True
dataEncipherment	X			S	False
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.8 Policy : 0.4.0.2042.1.7 Policy: 2.23.140.1.2.2
Extended Key Usage	X	False			
serverAuth	X			S	True
clientAuth	X			S	True
Certificate Transparency SCTs	X				Timestamp of the log servers.

E. TnTrust Gov CA End-Entity Certificates Profiles

The following types of Certificates are issued under TnTrust Gov CA:

1. Promosport certificate

Promosport Certificates are ETSI EN 319 411-1 Certificates not certified as generated on QSCD, with creation of the keys by the TunTrust RA, with 2048-bit key size and one (1) or two (2years validity from issuing start date.

These Certificates are compliant with the OID reference of the LCP certificate policy of the ETSI Technical Standard 319 411-1 (i.e., 0.4.0.2042.1.3).

The following table provides the description of the fields for Promosport Certificates issued under TnTrust Gov CA:

3 Additional SAN can be added depending on the subscriber requirement

Base Profile	Included	Critical	O/M[4]	CO[5]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Agency For Digital Certification, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
Locality	X		M	D	Locality Name
countryName	X		M	D	Nationality of holder (ISO3166)
emailAddress	X		M	D	Subject's email address
OrganizationName	X		M	D	Name of company/institution.
OrganizationalUnitName	X		O	D	Company department or other information item
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TunTrust Qualified CA public key
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.certification.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
KeyUsage	**X**	**True**			
digitalSignature	X			S	True
nonRepudiation	X			S	True
KeyEncipherment	X			S	True

4 O/M: O = Optional, M = Mandatory.

5 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

Extended Key Usage	X	False			
E-mail Protection	X			S	True
Client Authentication	X			S	True

2. UXP-eSeal Certificate

UXP eSeal Certificate is compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy and with 256 bits key size and two (2) years or one (1) month validity. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.9.1.9>.

The following table provides the description of the fields for UXP eSeal Certificates:

Base Profile	Included	Critical	O/M[6]	CO[7]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166)
OrganizationName	X		O	D	Contains the full registered name of the subject (legal person).
commonName	X		M	D	UXP Security server code
organisationIdentifier (2.5.4.97)	X		M	D	Contains information using the following structure in the presented order: - 3 character legal person identity type reference; VAT - 2 character ISO 3166 country code; - Hyphen-minus "-" and - Tax Identification number
BusinessCategory	X		M	S	GOV
serialNumber	X		O	D	UXP Security server code
Validity	X	False			
Not Before	X			D	Certificate generation process date/time

6 O/M: O = Optional, M = Mandatory.

7 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Not After	X			D	Certificate generation process date/time + 01 month or +02 years.
subjectPublicKeyInfo	X	False			
Algorithm	X				Id-ecPublicKey
SubjectPublicKey	X		M		256 bits
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
authorityInfoAccess	X	False			OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	False
nonRepudiation	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.9.1.9 Policy: 0.4.0.194112.1.3 Policy: 0.4.0.2042.1.2

3. UXP-ServerAuthentification Certificate

UXP Server Authentication Certificates are ETSI EN 319 411-1 Certificates and certified as generated on QSCD, with creation of the keys by the Subscriber, with 256-bit key size and one (1) month or one (1) year or two (2) years validity period starting from issuing start date.

The usage purpose of these certificates is the combined purpose of digital signature and key encryption. The UXP Server Authentication Certificates include the corresponding TunTrust OID for SSL server certificates, i.e., <2.16.788.1.2.6.9.1.8 >.

The following table provides the description of the fields for UXP Server Authentication Certificates issued under TnTrust Gov CA:

Base Profile	Included	Critical	O/M[8]	CO[9]	Values
Version	X	False		S	Version 3 Value=’2’
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption

8 O/M: O = Optional, M = Mandatory.

9 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA

Signature Value	X	False		D	TnTrust Gov CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Agency For Digital Certification, CN=TnTrust Gov CA
Subject DN	X	False			
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166)
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the incorporating or registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
serialNumber	X		M	D	Contains the Tax Identification number of the organization.
commonName	X		M	D	UXP Security server code
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 01 month or + 01 year or + 02 years.
subjectPublicKeyInfo	X	False			
Algorithm	X				Id-ecPublicKey
SubjectPublicKey	X		M		256 bits
X509v3 extensions					
X509v3 Authority Key Identifier	X				Keyid: 7B:D6:C4:15:45:CF:06:34:95:69:36:86:DA:75:7D:9B:FB:EB:73:D9
authorityInfoAccess	X	False			
Authority Information Access	X				CA Issuers – URI: http://www.tuntrust.tn/pub/TnTrustGovCA.crt OCSP – URI : http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI: http://crl.tuntrust.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA :FALSE
KeyUsage	X	True			

digitalSignature	X			S	True
nonRepudiation	X			S	True
KeyEncipherment	X			S	True
dataEncipherment	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy : 2.16.788.1.2.6.1.9.1.8
Extended Key Usage	X	False			
serverAuth	X			S	True
clientAuth	X			S	True

4. Digital Signature Certificate

Digital Signature Certificates follow the ETSI EN 319 411-1 standard and are not generated on a QSCD. The creation of the keys is done by TunTrust RA, with a 2048-bit key size and two (2) years validity period.

The following table provides the description of the fields for Digital Signature issued under TnTrust Gov CA:

Base Profile	Included	Critical	O/M[10]	CO[11]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	X		M	D	Given Name as on ID card
surname	X		M	D	Surname as on ID card without indication of 'épouse', 'ép' or similar.

10 O/M: O = Optional, M = Mandatory.

11 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

countryName	X		M	D	For certificates without professional attributes: This field contains the nationality of the holder (ISO3166). For certificates with professional attributes: This field contains the place of jurisdiction of the organization to which belongs the holder (ISO3166).
emailAddress	X		M	D	Subject's email address
OrganizationName	X		O	D	For certificate with professional attributes: Name of company/institution.
Organization Unit Name (OU)	X		O	D	**For natural person with professional attributes :** Contains information using the following structure in the presented order: - 2 character ISO 3166 country code; - hyphen-minus "-" and - Unique Identifier of the organization. **For natural person without professional attributes :** As constructed by CRAO
UID	X		M	D	This field contains the hash of the national ID number.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
authorityInfoAccess	X	False			CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustGovCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectAltName	X	False			
Rfc822Name	X		O	D	Certificate subscriber's email address
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
keyEncipherment	X			S	False

dataEncipherment	X			S	False
Extended Key Usage	X	False			
E-mail Protection	X			S	True
MS Smart Card Logon	X			S	True
Client Authentication	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9.1.5

5. Advanced DigiGO Certificate

Advanced DigiGO certificate is a QCP-n-qscd certificate policy with creation of the keys by TunTrust on a qualified cryptographic support (Hardware Security module) hosted by TunTrust, 2048 bit key size and forty five (45) days validity, and with a key usage limited to the support of advanced electronic signature. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.9.1.10>.

The following table provides the description of the fields for advanced DigiGO Certificates:

Base Profile	Included	Critical	O/M[12]	CO[13]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	X		M	D	Given Name as on ID card
surname	X		M	D	Surname as on ID card without indication of 'épouse', 'ép' or similar.
countryName	X		M	D	For certificates without professional attributes: This field contains the nationality of the holder (ISO3166). For certificates with professional attributes: This field contains the place of jurisdiction of the organization to which belongs the holder (ISO3166).
emailAddress	X		M	D	Subject's email address

12 O/M: O = Optional, M = Mandatory.

13 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

OrganizationName	X		O	D	For certificates with professional attributes: Name of organization.
Organization Unit Name (OU)	X		O	D	**For natural person with professional attributes :** Contains information using the following structure in the presented order: - 2 character ISO 3166 country code; - hyphen-minus "-" and - Unique Identifier of the organization. **For natural person without professional attributes :** As constructed by the operator
UID	X		M	D	This field contains the hash of the ID number.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 1 year
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
authorityInfoAccess	X	False			CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustGovCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectAltName	X	False			
Rfc822Name	X		O	D	Certificate subscriber's email address
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
keyEncipherment	X			S	False
dataEncipherment	X			S	False
Extended Key Usage	X	False			
E-mail Protection	X			S	True

MS Smart Card Logon	X			S	True
Client Authentication	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9.1.10 Policy: 0.4.0.194112.1.2

6. Entreprise-ID C40 Certificate

These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.11>.

The following table provides the description of the fields for Enterprise-ID C40 Certificates:

Base Profile	Included	Critical	O/M[14]	CO[15]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	ECDSA with SHA384
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	Contains the full registred name of the subject (legal person).
countryName	X		M	D	Country in which the company's or institution's registered office is established. (ISO3166)
organisationIdentifier (2.5.4.97)	X		M	D	Contains information using the following structure in the presented order: - 3-character legal person identity type reference; VAT - 2-character ISO 3166 country code; - hyphen-minus "-" and - Tax Identification number

14 O/M: O = Optional, M = Mandatory.

15 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

OrganizationName	X		M	D	Contains the full registered name of the subject (legal person).
OrganizationalUnitName	X		O	D	Company department or other information item.
Validity	X	False			
Not Before	X			D	Certificate generation process.
Not After	X			D	Certificate generation process date/time + 365 days or 730 days.
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 384 bits
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
authorityInfoAccess	X	False			OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.9.1.11 Policy: 0.4.0.194112.1.3 Policy:0.4.0.2042.1.2

7. VPN Certificate

The following table provides the description of the fields for VPN Certificates:

Base Profile	Included	Critical	O/M[16]	CO[17]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server or IP Address.
countryName	X		M	D	Nationality of holder. (ISO3166)
emailAddress	X		M	D	Subject's email address.
OrganizationName	X		M	D	Name of company/institution.
SubjectAltName	X	False			
SubjectAltName-DNSName[3]	X		O		FQDN (Fully Qualified Domain Name) of application/server – Exact and full URL for a Web Server or unique name of server.
SubjectAltName-IPAddress	X		O		IP address of the server.
Validity	X	False			
Not Before	X			D	Certificate generation process.

16 O/M: O = Optional, M = Mandatory.

17 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Not After	X			D	Certificate generation process date/time + 365 days or 730 days.
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
KeyUsage	X	True			
digitalSignature	X			S	True
KeyAgreement	X			S	True
KeyEncipherment	X			S	True
Extended Key Usage	X	False			
IPSec End System	X			S	True
IPSec User	X			S	True
IPSec Tunnel	X			S	True

8. National Backend TLS Client Authentication Certificate

The creation of this certificate profile is part of the "pass-sanitaire" project. The following table provides the description of the fields for National Backend TLS Client Authentication Certificates:

Base Profile	**Included**	**Critical**	**O/M[18]**	**CO[19]**	**Values**
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates

18 O/M: O = Optional, M = Mandatory.
19 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Signature Algorithm					
Algorithm	X	False		S	SHA256 with RSA
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Agency For Digital Certification, CN=TnTrust Gov CA
Subject DN	X	False			
commonName	X		M	D	non-empty and unique common name
countryName	X		M	D	TN
OrganizationName	X		M	D	Name of company/institution.
Validity	X	False			
Not Before	X			D	Certificate generation process.
Not After	X			D	Certificate generation process date/time + 730 days.
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Gov CA public key
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/ tntrustgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
KeyUsage	X	True			
digitalSignature	X			S	True
Extended Key Usage	X	False			
Client Authentication	X				True

F. TnTrust Qualified Gov CA End-Entity Certificates Profiles

The following types of Certificates are issued under TnTrust Qualified Gov CA :

1. ID-Trust Certificate

ID-Trust is a Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the TunTrust on a qualified cryptographic support (token or Hardware Security module), 2048 bit key size and two (2) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.1>.

The following table provides the description of the fields for ID-Trust Certificates:

Base Profile	Included	Critical	O/M[20]	C[21]O	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	X		M	D	Given Name as on ID card
surname	X		M	D	Surname as on ID card without indication of 'épouse', 'ép' or similar.
countryName	X		M	D	For certificates without professional attributes: This field contains the nationality of the holder (ISO3166). For certificates with professional attributes: This field contains the place of jurisdiction of the organization to which belongs the holder (ISO3166).
emailAddress	X		M	D	Subject's email address
OrganizationName	X		O	D	For certificate with professional attributes: Name of company/institution.
Organization Unit Name (OU)	X		O	D	**For natural person with professional attributes :** Contains information using the following structure in the presented order: - 2 character ISO 3166 country code; - hyphen-minus "-" and - Unique Identifier of the organization. **For natural person without professional attributes :** As constructed by CRAO
UID	X		M	D	This field contains the hash of the national ID number.
Validity	X	False			

[20] O/M: O = Optional, M = Mandatory.

[21] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Qualified Gov CA public key
authorityInfoAccess	X	False			CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustQualifiedGovCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
subjectAltName	X	False			
Rfc822Name	X		O	D	Certificate subscriber's email address
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
keyEncipherment	X			S	False
dataEncipherment	X			S	False
Extended Key Usage	X	False			
E-mail Protection	X			S	True
MS Smart Card Logon	X			S	True
Client Authentication	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.10.1.1 Policy: 0.4.0.194112.1.2
QualifiedCertificateStat	X	False			
QcCompliance (0.4.0.1862.1.1)	X		M	S	True
QcSSCD (0.4.0.1862.1.4)			M	S	True
QcPDS (0.4.0.1862.1.5)	X		M	S	http://www.certification.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X		M	S	Id-etsi-qct-esign (0.4.0.1862.1.6.1)

2. Enterprise-ID Certificate

Enterprise-ID is a qualified Certificate compliant with ETSI EN 319 411-2 QCP-l-qscd certificate policy with creation of the keys by the TunTrust on a qualified cryptographic support (token or Hardware Security module), 2048 bit key size and two (2) years validity, and with a key usage limited to the support of qualified e-seal. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.2>.

The following table provides the description of the fields for Enterprise-ID Certificates:

Base Profile	Included	Critical	O/M[22]	CO[23]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TunTrust Qualified Gov CA
Subject DN	X	False			
commonName	X		M	D	Contains the full registred name of the subject (legal person)
countryName	X		M	D	Country in which the company's or institution's registered office is established. (ISO3166)
organisationIdentifier (2.5.4.97)	X		M	D	Contains information using the following structure in the presented order: - 3-character legal person identity type reference; VAT - 2-character ISO 3166 country code; - hyphen-minus "-" and - Tax Identification number
OrganizationName	X		M	D	Contains the full registered name of the subject (legal person).
OrganizationalUnitName	X		O	D	Company department or other information item
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TunTrust Qualified Gov CA public key
authorityInfoAccess	X	False			OCSP - URI:http://va.tuntrust.tn

[22] O/M: O = Optional, M = Mandatory.

[23] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.10.1.2 Policy: 0.4.0.194112.1.3 Policy:0.4.0.2042.1.2
QualifiedCertificateStat	X	False			
QcCompliance (0.4.0.1862.1.1)	X		M	S	True
QcSSCD (0.4.0.1862.1.4)			M	S	True
QcPDS (0.4.0.1862.1.5)	X		M	S	http://www.certification.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X		M	S	Id-etsi-qct-eseal (0.4.0.1862.1.6.2)

3. DigiGO Certificate

DigiGO is a Qualified Certificate compliant with ETSI EN 319 411-2 QCP-n-qscd certificate policy with creation of the keys by the TunTrust on a qualified cryptographic support (Hardware Security module) hosted by TunTrust, 2048 bit key size and two (2) years validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the corresponding TunTrust OID, i.e., < OID 2.16.788.1.2.6.1.10.1.3>.

The following table provides the description of the fields for DigiGO Certificates:

Base Profile	Included	Critical	O/M[24]	CO[25]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	C=TN, L=Tunis, O=National Digital Certification Agency, CN=TnTrust Qualified Gov CA
Subject DN	X	False			
commonName	X		M	D	Concatenation of given name and surname as in ID card separated by a "space" character.
givenName	X		M	D	Given Name as on ID card
surname	X		M	D	Surname as on ID card without indication of 'épouse', 'ép' or similar.
countryName	X		M	D	For certificates without professional attributes: This field contains the nationality of the holder (ISO3166). For certificates with professional attributes: This field contains the place of jurisdiction of the organization to which belongs the holder (ISO3166).
emailAddress	X		M	D	Subject's email address
OrganizationName	X		O	D	For certificates with professional attributes: Name of organization.
Organization Unit Name (OU)	X		O	D	**For natural person with professional attributes :** Contains information using the following structure in the presented order: - 2 character ISO 3166 country code; - hyphen-minus "-" and - Unique Identifier of the organization. **For natural person without professional attributes :** As constructed by the operator
UID	X		M	D	This field contains the hash of the ID number.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time

[24] O/M: O = Optional, M = Mandatory.

[25] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TnTrust Qualified Gov CA public key
authorityInfoAccess	X	False			CA Issuers - URI:http://www.tuntrust.tn/pub/TnTrustQualifiedGovCA.crt OCSP - URI:http://va.tuntrust.tn
X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
subjectAltName	X	False			
Rfc822Name	X		O	D	Certificate subscriber's email address
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
Policy Properties					
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
keyEncipherment	X			S	False
dataEncipherment	X			S	False
Extended Key Usage	X	False			
E-mail Protection	X			S	True
MS Smart Card Logon	X			S	True
Client Authentication	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.10.1.3 Policy: 0.4.0.194112.1.2
QualifiedCertificateStat	X	False			
QcCompliance (0.4.0.1862.1.1)	X		M	S	True
QcSSCD (0.4.0.1862.1.4)			M	S	True
QcPDS (0.4.0.1862.1.5)	X		M	S	http://www.tuntrust.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X		M	S	Id-etsi-qct-esign (0.4.0.1862.1.6.1)

4. Mobile-ID Certificate

Mobile-ID is a Qualified Certificate where Key Pair are generated by TunTrust on a qualified cryptographic support (Hardware Security module) hosted by TunTrust, having a 2048-bit key size and one (1) year validity, and with a key usage limited to the support of qualified electronic signature. These Certificates include the following TunTrust OID: < OID 2.16.788.1.2.6.1.10.1.4>.

The following table provides the description of the fields for Mobile-ID Certificates:

Base Profile	Included	Critical	O/M[26]	CO[27]	Values
Version	X	False	M	S	3 (0x2)
Serial Number	X	False	M	FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False	M	S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature value	X	False	M	D	Issuing CA signature
Issuer DN	X	False	M	S	CN = TnTrust Qualified Gov CA O = National Digital Certification Agency L = Tunis C = TN
Validity					
Not Before	X	False	M	D	Certificate generation process date/time.
Not After	X	False	M	D	Certificate generation process date/time + one (01) year.
Subject DN					
CN, commonName	X	False	M	D	Concatenation of the given name and surname in the Arabic Language as on Tunisian National ID card, separated by a space character without indication of 'حرم', 'بنت' or similar.
givenName	X	False	M	D	Given name in the Arabic Language as on Tunisian National ID card without indication of 'حرم', 'بنت' or similar.
surname	X	False	M	D	Surname in the Arabic Language as on Tunisian National ID card.
UID	X	False	M	D	ID number generated by CNI – IT Ministry.
C, countryName	X	False	M	D	Nationality of the holder (ISO3166).
Subject public key info					
Public key algorithm	X	False	M	S	RSA Exponent: 65537 (0x10001)
Public key	X	False	M	S	2048 bits

[26] O/M: O = Optional, M = Mandatory.

[27] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

specifications					
X509v3 extensions					
Authority Information Access	X	False	M	S	CA Issuers - URI : http://www.tuntrust.tn/pub/TnTrustQualifiedGovCA.crt OCSP - URI: http://va.tuntrust.tn
X509v3 Subject Key Identifier	X	False	M	D	SHA-1 hash of subject public key
X509v3Authority Key Identifier	X	False	M	S	SHA-1 hash of TnTrust Qualified Gov CA public key
X509v3 Basic Constraints	X	True	M	S	CA : FALSE
X509v3 Certificate Policies	X	False	M	S	Policy : 2.16.788.1.2.6.1.10.1.4 Policy : 0.4.0.194112.1.2 Policy : 0.4.0.2042.1.2
X509v3 CRL distribution Points	X	False	M	S	URI: http://crl.tuntrust.tn/tntrustqualifiedgovca.crl
X509v3 Key Usage	X	True	M	S	Digital Signature, Non-repudiation
X509v3 Extended Key Usage	X	False	M	S	Client Authentication, MS Smart Card Logon, E-mail protection
Qualified Certificate Stat					
QcCompliance (0.4.0.1862.1.1)	X	False	M	S	True
QcSSCD (0.4.0.1862.1.4)		False	M	S	True
QcPDS (0.4.0.1862.1.5)	X	False	M	S	http://www.certification.tn/pub/pds-tuntrustgovca.pdf
QcType (0.4.0.1862.1.6)	X	False	M	S	Id-etsi-qct-esign (0.4.0.1862.1.6.1)

G. TN01 End-Entity Certificates Profiles

The following type of Certificates is issued under TN01 CA:

1. 2D-DOC Certificate

The following table provides the description of the fields for 2D-DOC Certificates:

Base Profile	Included	Critical	O/M[28]	CO[29]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	ecdsa-with-SHA384

28 O/M: O = Optional, M = Mandatory.

29 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

Signature Value	X	False		D	TN01 Signature
Issuer DN	X			S	CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Subject DN	X	False			
commonName	X		M	D	04 characters (as assigned bu CRAO)
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
OrganizationalUnitName	X		O	D	Tax Identifier of the Organization
emailAddress	X		O	D	The email Address of the responsible of the seal.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + number of days ≤ 730 days (2 years)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				keyid: CE:87:48:48:A9:2F:A8:F5:B6:CB:F7:97:B5:F7:02:91:D2:8A:9C:58
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI: URI:http://crl.certification.tn/cevca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
nonRepudiation	X			S	True
dataEncipherment	X			S	False
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 2.16.788.1.2.6.1.12

2. Upload Certificate

The creation of this certificate profile is part of the "pass-sanitaire" project. The following table provides the description of the fields for Upload Certificates:

Base Profile	Included	Critical	O/M[30]	CO[31]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	SHA256 with ECDSA
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	CN=TN01, OU=TN CEV CA, O=National Digital Certification Agency, C=TN
Subject DN	X	False			
commonName	X		M	D	non-empty and unique common name
countryName	X		M	D	TN
OrganizationName	X		M	D	Name of company/institution.
Validity	X	False			
Not Before	X			D	Certificate generation process.
Not After	X			D	Certificate generation process date/time + 730 days.
X509v3 extensions					
X509v3 Authority Key Identifier	X				SHA-1 hash of TN01 public key
authorityInfoAccess	X	False			
Authority Information Access	X				CA Issuers - URI:http://www.tuntrust.tn/pub/TN01.crt OCSP - URI:http://va.certification.tn

[30] O/M: O = Optional, M = Mandatory.

[31] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

X509v3 CRL Distribution Points	X	False		S	URI:http://crl.tuntrust.tn/cevca.crl
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
KeyUsage	X	True			
digitalSignature	X			S	True

H. CSCA TUNISIA DGC End-Entity Certificates Profiles

The following type of Certificates is issued under CSCA TUNISIA DGC:

1. DSC certificate profile:

Base Profile	Critical	Values
Version		3 (0x2)
Serial Number		To be defined
Signature Algorithm		ecdsa-with-SHA256
Issuer		CN=CSCA TUNISIA DGC O=AGENCE NATIONALE DE CERTIFICATION ELECTRONIQUE C=TN
Subject		CN= CENTRE INFORMATIQUE DU MINISTERE DE LA SANTE PUBLIQUE, O= CENTRE INFORMATIQUE DU MINISTERE DE LA SANTE PUBLIQUE, C=TN
Validity		
Not Before		Issuance date
Not After		Issuance date + **2 years**
X509v3 Private Key Usage Period		Not Before: issuance date, Not After: issuance date + 6 months
Subject Pubic Key Info		
Public Key Algorithm		id-ecPublicKey
id-ecPublicKey		256 bit
pub		To be identified
X509v3 extensions		
X509v3 Subject Key Identifier		To be identified
X509v3 Authority Key Identifier		To be identified
X509v3 Basic Constraints	True	CA: False
X509 Key Usage	True	Digital Signature
Authority Information Access		CA Issuers - URI: http://www.tuntrust.tn/pub/cscatndgc.crt

X509 CRL Distribution Points		URI: http://www.tuntrust.tn/cscatndgc.crl
X509v3 Extended Key Usage		OID 1.3.6.1.4.1.0.1847.2021.1.1 -- valid for test OID 1.3.6.1.4.1.0.1847.2021.1.2 -- valid for vaccinations OID 1.3.6.1.4.1.0.1847.2021.1.3 -- valid for recovery

I. TimeStamp certificate

The following table provides the description of the fields for Timestamp Certificates issued to TunTrust timestamp unit:

Base Profile	Included	Critical	O/M[32]	CO[33]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the Timestamp Unit
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 1095 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI:URI of the CRL
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
certificatePolicies	X	False			

32 O/M: O = Optional, M = Mandatory.

33 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9.1.7
Extended Key Usage	X	False			
Time Stamping	X			S	True

J. OCSP Certificate

The following table provides the description of the fields for TunTrust OCSP profile:

Base Profile	Included	Critical	O/M[34]	CO[35]	Values
Version	X	False		S	Version 3 Value='2'
Serial Number	X	False		FDV	Validated on duplicates
Signature Algorithm					
Algorithm	X	False		S	OID: 1.2.840.113549.1.1.11 SHA256 with RSA Encryption
Signature Value	X	False		D	Issuing CA Signature
Issuer DN	X			S	Issuing CA DN
Subject DN	X	False			
commonName	X		M	D	Name of the validation Authority
countryName	X		M	D	Country in which the company's or institution's registered office is established (ISO3166).
OrganizationName	X		M	D	Contains the full registered name of the organization as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA.
Locality	X		M	D	Locality Name
Validity	X	False			
Not Before	X			D	Certificate generation process date/time
Not After	X			D	Certificate generation process date/time + 730 days
subjectPublicKeyInfo	X	False			
Algorithm	X				Public Key: Key length: 2048 bits (RSA) Exponent: 65537 (0x10001)
SubjectPublicKey	X		M		
X509v3 extensions					
X509v3 Authority Key Identifier	X				Authority Key Identifier
authorityInfoAccess	X	False			
Authority Information Access	X				OCSP - URI:http://va.certification.tn
X509v3 CRL Distribution Points	X	False		S	URI:URI of the CRL
subjectKeyIdentifier	X	False			
keyIdentifier	X				This extension identifies the public key being certified.
X509v3 Basic Constraints	X	True			CA : FALSE
KeyUsage	X	True			
digitalSignature	X			S	True
certificatePolicies	X	False			
PolicyIdentifier	X				Policy: 0.4.0.2042.1.2 Policy: 2.16.788.1.2.6.1.9
OCSP No Check	X			S	
Extended Key Usage	X	False			
OCSP Signing	X			S	True

K. CRL profile

34 O/M: O = Optional, M = Mandatory.

35 CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

In conformance with the IETF PKIX RFC 2459, the TunTrust CAs support CRLs compliant with:

- Version numbers supported for CRLs
- CRL and CRL entry extensions populated and their criticality.

The profile of the CRL is provided in the table below:

Field	Value
Version	V2 in accordance with RFC 5280.
Signature Algorithm	Object identifier of the algorithm used to sign the certificate sha256RSA.
Issuer DN	Subject CA
ThisUpdate	Issue date/time of the CRL. CRLs are effective upon issuance.
NextUpdate	Date by which the next CRL will be issued. Creation date/time + 365 days for Offline CA Creation date/time + 6 days for Online Issuing CA
revokedCertificates	
userCertificate	Certificate serial number
revocationDate	Revocation time
crlExtensions	
CRL Number	A monotonically increasing sequence number in accordance with RFC 5280
Authority Key Identifier	Populated by CA application contains key id (SHA1) of issuer public key
2.5.29.60	True This field is only activated for TnTrust Qualified Gov CA.

L. Timestamp Request Format

The following table lists the fields that are expected by the Time Stamping units:

Field	Value / Comment
Document Hash	Hash of the document on which the TimeStamp must be computed
Hash OID	SHA-256
Nonce	A random number, also referred to as “nonce”, allows the developer to better associate a Timestamp Request to its response, since the latter will include the same nonce.
Should TSA Certificate be included?	True/False

M. Timestamp Response Format

The following table lists which fields are populated by the Time Stamping units:

Field	Value / Comment

Generation Time	The Time at which the time-stamp token has been created by the TSA. It is expressed as UTC time (Coordinated Universal Time).
Document Hash	Hash of the document on which the TimeStamp response has been computed.
Hash algorithm	SHA-256
Policy OID	2.16.788.1.2.6.1.11 The OID of the policy that should be applied by the TSU during the generation of the timestamp token. The policy generally describes legal value and accuracy of the resulting timestamp.
Accuracy	1 second
TSA Certificate Information	Current TSU Certificate
QcStatement	True